# On sets of large exponential sums, I *

Shkredov I.D.

Annotation.

*Let $A$ be a subset of $\mathbb{Z}/N\mathbb{Z}$ and let $\mathcal{R}$ be the set of large Fourier coefficients of $A$. Properties of $\mathcal{R}$ have been studied in works of M.– C. Chang and B. Green. Our result is the following : the number of quadruples $(r_1, r_2, r_3, r_4) \in \mathcal{R}^4$ such that $r_1 + r_2 = r_3 + r_4$ is at least $|\mathcal{R}|^{2+\epsilon}, \epsilon > 0$. This statement shows that the set $\mathcal{R}$ is highly structured. We also discuss some of the generalizations and applications of our result.*

**1. Introduction.**

Let $N$ be a positive integer. By $\mathbb{Z}_N$ denote the set $\mathbb{Z}/N\mathbb{Z}$. Let $f : \mathbb{Z}_N \to \mathbb{C}$ be an arbitrary function. Denote by $\widehat{f}$ the Fourier transform of $f$

$$\widehat{f}(r) = \sum_{n \in \mathbb{Z}_N} f(n) e(-nr)\,, \qquad (1)$$

where $e(x) = e^{-2\pi i x/N}$. By Parseval's identity

$$\sum_{r \in \mathbb{Z}_N} |\widehat{f}(r)|^2 = N \sum_{x \in \mathbb{Z}_N} |f(x)|^2\,. \qquad (2)$$

Let $\delta, \alpha$ be real numbers, $0 < \alpha \leq \delta \leq 1$ and let $A$ be a subset of $\mathbb{Z}_N$ of cardinality $\delta N$. It is very convenient to write $A(x)$ for such a function. Thus $A(x) = 1$ if $x \in A$ and $A(x) = 0$ otherwise. Consider the set $\mathcal{R}_\alpha$ of large exponential sums of the set $A$

$$\mathcal{R}_\alpha = \mathcal{R}_\alpha(A) = \{\ r \in \mathbb{Z}_N\ :\ |\widehat{A}(r)| \geq \alpha N\ \}\,. \qquad (3)$$

In many problems of combinatorial number theory is important to know the structure of the set $\mathcal{R}_\alpha$ (see [1]). In other words what kind of properties $\mathcal{R}_\alpha$ has?

It is easy to see that $0 \in \mathcal{R}_\alpha$ and $\mathcal{R}_\alpha = -\mathcal{R}_\alpha$. Further, using (2) we obtain $|\mathcal{R}_\alpha| \leq \delta/\alpha^2$. Are there any non–trivial properties of the set $\mathcal{R}_\alpha$?

In 2002 M.– C. Chang proved the following result [3].

**Theorem 1.1 (Chang)** *Let $\delta, \alpha$ be real numbers, $0 < \alpha \leq \delta \leq 1$, $A$ be a subset of $\mathbb{Z}_N$, $|A| = \delta N$. Then there exists a set $\Lambda = \{\lambda_1, \dots, \lambda_{|\Lambda|}\} \subseteq \mathbb{Z}_N$, $|\Lambda| \leq 2(\delta/\alpha)^2 \log(1/\delta)$ such that for any $r \in \mathcal{R}_\alpha$ we have*

$$r = \sum_{i=1}^{|\Lambda|} \varepsilon_i \lambda_i \pmod N\,, \qquad (4)$$

*This work was supported by RFFI grant no. 06-01-00383, President's of Russian Federation grant N 1726.2006.1 and INTAS (grant no. 03–51–5-70).

*where* $\varepsilon_i \in \{-1,0,1\}$.

Using approach of paper [4] (see also [5]) Chang applied her result to prove the famous Freiman's theorem [6] on sets with small doubling. Let us formulate this beautiful result.

The set $Q \subseteq \mathbb{Z}$

$$Q = \{n_0 + n_1\lambda_1 + \cdots + n_d\lambda_d \ : \ 0 \le \lambda_i < m_i\}$$

is said to be a *d–dimensional arithmetic progression.*

**Theorem 1.2 (Freiman)** *Let $C > 0$ be a real number and $A \subseteq \mathbb{Z}$ be an arbitrary set. Suppose that $|A+A| \le C|A|$. Then there exist numbers $d$ and $K$ depend on $C$ only and a $d$–dimensional arithmetic progression $Q$ such that $|Q| \le K|A|$ and $A \subseteq Q$.*

The second application of Theorem 1.1 was obtained by B. Green in paper [7] (see also [11, 12] and [13]). Let us formulate one of the main results of [7].

**Theorem 1.3 (Green)** *Let $A$ be an arbitrarily subset of $\mathbb{Z}_N$, $|A| = \delta N$. Then $A+A+A$ contains an arithmetic progression of length at least*

$$2^{-24}\delta^5(\log(1/\delta))^{-2}N^{\delta^2/250\log(1/\delta)}\,. \qquad (5)$$

In paper [8] Green showed that Chang's theorem is sharp in a certain sense. Let $E = \{e_1,\ldots,e_{|E|}\} \subseteq \mathbb{Z}_N$ be an arbitrary set. By $\mathrm{Span}(E)$ denote the set of all sums $\sum_{i=1}^{|E|}\varepsilon_i e_i$, where $\varepsilon_i \in \{-1,0,1\}$.

**Theorem 1.4 (Green)** *Let $\delta, \alpha$ be real numbers, $\delta \le 1/8$, $0 < \alpha \le \delta/32$. Let also*

$$\left(\frac{\delta}{\alpha}\right)^2 \log(1/\delta) \le \frac{\log N}{\log\log N}\,. \qquad (6)$$

*Then there exists a set $A \subseteq \mathbb{Z}_N$, $|A| = [\delta N]$ such that the set $\mathcal{R}_\alpha$ does not contain in $\mathrm{Span}(\Lambda)$ for any set $\Lambda$ of cardinality $2^{-12}(\delta/\alpha)^2\log(1/\delta)$.*

If the parameter $\alpha$ is close to $\delta$ then the structural properties of the set $\mathcal{R}_\alpha$ was studied in papers [14, 15, 16], see also survey [17].

The main result of the paper is the following theorem.

**Theorem 1.5** *Let $\delta, \alpha$ be real numbers, $0 < \alpha \le \delta$, $A$ be a subset of $\mathbb{Z}_N$, $|A| = \delta N$ and $k \ge 2$ Suppose that $B \subseteq \mathcal{R}_\alpha \setminus \{0\}$ is an arbitrary set. Then the number*

$$T_k(B) := |\{\ (r_1,\ldots,r_k,r'_1,\ldots,r'_k) \in B^{2k} \ : \ r_1+\cdots+r_k = r'_1+\cdots+r'_k\ \}| \qquad (7)$$

*is at least*

$$\frac{\delta\alpha^{2k}}{2^{4k}\delta^{2k}}|B|^{2k}\,. \qquad (8)$$

Let us show that the statement of Theorem 1.5 is not trivial in the case when $\delta$ tends to zero as $N$ tends to infinity (if $\delta$ does not tends to zero as $N \to \infty$ then there are not non–trivial restrictions on structure of the set $\mathcal{R}_\alpha$, see papers [18, 19, 20]). Let us consider the simplest case $k = 2$. Let the cardinality of $\mathcal{R}_\alpha$ is equal to $\Theta(\delta/\alpha^2)$. Using Theorem 1.5, we obtain that the number of solutions of the equation

$$r_1 + r_2 = r_3 + r_4\,, \qquad \text{where} \qquad r_1,r_2,r_3,r_4 \in \mathcal{R}_\alpha \setminus \{0\} \qquad (9)$$

equals $\Theta(\delta/\alpha^4)$. There are three sorts of trivial solutions of equation (9). The first sort of solutions is $r_1 = r_3$, $r_2 = r_4$, the second — $r_1 = r_4$, $r_2 = r_3$, and the third — $r_1 = -r_2$,

$r_3 = -r_4$. So the number of trivial solutions of (9) does not exceed $3|\mathcal{R}_\alpha|^2$. Since the cardinality of $\mathcal{R}_\alpha$ does not exceed $\delta/\alpha^2$ it follows that $3|\mathcal{R}_\alpha|^2$ at most $3\delta^2/\alpha^4$. This number is less than $\delta/\alpha^4$ as $\delta$ tends to zero. Thus Theorem 1.5 asserts that equation (9) has non–trivial solutions. In the sense Theorem 1.5 shows that the set $\mathcal{R}_\alpha$ has some additive structure.

We prove Theorem 1.5 in section 2. In §3 we obtain a matrix generalization of our approach. We use Gowers uniformity norms (see [2]) in our proof.

In section 4 we obtain some applications of our main result. We show that Theorem and W. Rudin's inequality implies Chang's result. Moreover we derive an improvement of Theorem 1.1 (see Theorem 4.3). Also we obtain an application of Theorem 1.5 to Freiman's Theorem 1.2.

In our forthcoming papers we are going to obtain further results on sets of large exponential sums.

The author is grateful to Professor S.V. Konyagin for his helpful idea and to N.G. Moshchevitin for constant attention to this work.

**2. Proof of main result.**

Let us explain the main idea of the proof of Theorem 1.5. Let $N$ be a positive integer and $\widehat{A}(r)$ the Fourier transform of the characteristic function of a set $A$. As was noted above, we have Parseval's identity

$$\sum_{r\in\mathbb{Z}_N} |\widehat{A}(r)|^2 = N|A|\,. \tag{10}$$

Are there another relationships between Fourier coefficients $\widehat{A}(r)$? It is easy to see that the answer is yes.

Let us consider a slightly more general situation. Let $f : \mathbb{Z}_N \to \mathbb{C}$ be a complex function. We have the inversion formula

$$f(x) = \frac{1}{N}\sum_{r\in\mathbb{Z}_N} \widehat{f}(r)e(rx)\,. \tag{11}$$

The function $f(x)$ is the characteristic function of a subset of $\mathbb{Z}_N$ iff for any $x \in \mathbb{Z}_N$ we have

$$|f(x)|^2 = f(x)\,. \tag{12}$$

Combining (11) and (12), we get

$$\frac{1}{N^2}\sum_{r',r''} \widehat{f}(r')\overline{\widehat{f}(r'')}e(r'x - r''x) = \frac{1}{N}\sum_{u} \widehat{f}(u)e(ux)\,. \tag{13}$$

Hence

$$\sum_{u}\left(\frac{1}{N}\sum_{r} \widehat{f}(r)\overline{\widehat{f}(r-u)}\right)e(ux) = \sum_{u} \widehat{f}(u)e(ux)\,. \tag{14}$$

Identity (14) is true for all $x \in \mathbb{Z}_N$. It follows that

$$\widehat{f}(u) = \frac{1}{N}\sum_{r} \widehat{f}(r)\overline{\widehat{f}(r-u)}\,. \tag{15}$$

Thus the complex function $f : \mathbb{Z}_N \to \mathbb{C}$ is the characteristic function iff identity (15) holds. Moreover, (15) contains all relationships between Fourier coefficients of the set $A$. For example to obtain Parseval's identity (2) one can put $u = 0$ in formula (15).

We need in an obvious generalization of (15). Suppose that $f, g : \mathbb{Z}_N \to \mathbb{C}$ are two complex functions. Then

$$\frac{1}{N}\sum_r \widehat{f}(r)\overline{\widehat{g}(r-u)} = \sum_x f(x)\overline{g(x)}e(-xu)\,. \qquad (16)$$

Clearly, (16) implies (15).

Let us explian the main idea of our proof. Let $A \subseteq \mathbb{Z}_N$ be a set, $|A| = \delta N$, and $\mathcal{R}_\alpha$ be the set of large exponential sums of $A$. Let us consider the model situation. Suppose that for all $r \in \mathcal{R}_\alpha \setminus \{0\}$ we have $|\widehat{A}(r)| = \alpha N$, and if $r \notin \mathcal{R}_\alpha$, $r \neq 0$ it follows that $\widehat{A}(r) = 0$ (we shall explain this assumption later). Let $\delta \leq 1/4$, and $0 \neq u \in \mathcal{R}_\alpha$ be an arbitrary residual. By assumtion $|\widehat{A}(u)| = \alpha N$. Using (15) and the triangle inequality, we get

$$\alpha N = |\widehat{A}(u)| \leq \frac{1}{N}\sum_r |\widehat{A}(r)||\widehat{A}(r-u)| \leq$$

$$\leq \frac{1}{N}\delta N|\widehat{A}(-u)| + \frac{1}{N}|\widehat{A}(u)|\delta N + \frac{1}{N}\sum_{r\neq 0, r\neq u} |\widehat{A}(r)||\widehat{A}(r-u)|\,. \qquad (17)$$

It follows that

$$\frac{1}{N}\sum_{r\neq 0, r\neq u} |\widehat{A}(r)||\widehat{A}(r-u)| \geq \frac{\alpha N}{2}\,.$$

For all $r \neq 0$ we have $|\widehat{A}(r)| = \alpha N \cdot \mathcal{R}_\alpha(r)$. Hence

$$\sum_{r\neq 0, r\neq u} \mathcal{R}_\alpha(r)\mathcal{R}_\alpha(r-u) \geq \frac{1}{2\alpha}\,. \qquad (18)$$

Using (18), we obtain for all $u \in \mathcal{R}_\alpha \setminus \{0\}$ the number of solution of the equation $r_1 - r_2 = u$, where $r_1, r_2 \in \mathcal{R}_\alpha \setminus \{0\}$ is at least $1/(2\alpha)$. Therefore there are non–trivial arithmetic relationships between the elements of the set $\mathcal{R}_\alpha$.

Let us give a strict proof of Theorem 1.5. To show the main idea of the proof we deduce our result for the simplest case $k = 2$ and after that in full generality. Thus let $k = 2$, and $B$ be an arbitrary subset of $\mathcal{R}_\alpha \setminus \{0\}$. By $[N]$ denote the segment of positive integers $\{1, 2, \ldots, N\}$.

We need in the following lemma.

**Lemma 2.1** *Let $\delta, \alpha'$ be real numbers, $0 < \alpha' \leq \delta$ and $A$ be a subset of $\mathbb{Z}_N$, $|A| = \delta N$. Let also*

$$\mathcal{R}'_{\alpha'} = \{\ r \in \mathbb{Z}_N\ :\ \alpha' N \leq |\widehat{A}(r)| < 2\alpha' N\ \} \qquad (19)$$

*and $B'$ be an arbitrary subset of $\mathcal{R}'_{\alpha'} \setminus \{0\}$. Then $T_2(B') \geq (\alpha')^4|B'|^4/(16\delta^3)$.*

**Proof.** Let

$$f_{B'}(x) = \frac{1}{N}\sum_{r\in B'} \widehat{A}(r)e(rx)\,.$$

It is easy to see that $\widehat{f}_{B'}(r) = \widehat{A}(r)B'(r)$. Let

$$\sigma = \sum_s |\sum_r \widehat{f}_{B'}(r)\overline{\widehat{A}(r-s)}|^2\,. \qquad (20)$$

Using (16) and Parseval's identity, we get

$$\sigma = N^2\sum_s |\sum_x f_{B'}(x)\overline{A(x)}e(-xs)|^2 = N^3\sum_x |f_{B'}(x)|^2 A(x)^2\,. \qquad (21)$$

Let us obtain a lower bound for $\sum_x |f_{B'}(x)|^2 A(x)^2$. Using (2) and the definition of the set $\mathcal{R}'_{\alpha'}$, we have

$$\left(\sum_x f_{B'}(x)A(x)\right)^2 = \left(\frac{1}{N}\sum_r \widehat{f}_{B'}(r)\overline{\widehat{A}(r)}\right)^2 = \left(\frac{1}{N}\sum_r |\widehat{f}_{B'}(r)|^2\right)^2 \geq \tag{22}$$

$$\geq (N\alpha'^2|B'|)^2 = \alpha'^4|B'|^2N^2\,. \tag{23}$$

On the other hand

$$\left(\sum_x f_{B'}(x)A(x)\right)^2 \leq \left(\sum_x |f_{B'}(x)|^2A(x)^2\right)\cdot\left(\sum_x A(x)^2\right) = \delta N\left(\sum_x |f_{B'}(x)|^2A(x)^2\right). \tag{24}$$

Using (23) and (24), we obtain

$$\sigma^2 \geq \frac{\alpha'^8}{\delta^2}|B'|^4N^8\,. \tag{25}$$

Let us obtain an upper bound for $\sigma^2$. We have

$$\sigma = \sum_s\sum_{r,r'} \widehat{f}_{B'}(r)\overline{\widehat{f}_{B'}(r')}\cdot\overline{\widehat{A}(r-s)}\widehat{A}(r'-s) =$$

$$= \sum_u\left(\sum_r \widehat{f}_{B'}(r)\overline{\widehat{f}_{B'}(r-u)}\right)\cdot\overline{\left(\sum_r \widehat{A}(r)\overline{\widehat{A}(r-u)}\right)}\,. \tag{26}$$

It follows that

$$\sigma^2 \leq \sum_u\left|\sum_r \widehat{f}_{B'}(r)\overline{\widehat{f}_{B'}(r-u)}\right|^2\cdot\sum_u\left|\sum_r \widehat{A}(r)\overline{\widehat{A}(r-u)}\right|^2 = \sigma_1\cdot\sigma_2\,. \tag{27}$$

Using (15) and Parseval's identity, we get

$$\sigma_2 = N^2\sum_u |\widehat{A}(u)|^2 = \delta N^4\,. \tag{28}$$

Since $\widehat{f}_{B'}(r) = \widehat{A}(r)B'(r)$ and $B' \subseteq \mathcal{R}'_{\alpha'} \setminus \{0\}$ it follows that $|\widehat{f}_{B'}(r)| \leq 2\alpha' B'(r)N$. Hence

$$\sigma_1 \leq 16(\alpha')^4T_2(B')N^4\,. \tag{29}$$

Combining (28), (29) and (25), we obtain $T_2(B') \geq (\alpha')^4|B'|^4/(16\delta^3)$. This completes the proof of Lemma 2.1.

Let

$$B_i = \{\ r \in B\ :\ \alpha 2^{i-1}N \leq |\widehat{A}(r)| < \alpha 2^iN\ \}\,,\quad i \geq 1\,.$$

Clearly, $B = \bigsqcup_{i\geq 1} B_i$. Using Lemma 2.1, we obtain $T_2(B_i) \geq (\alpha 2^{i-1})^4|B_i|^4/(16\delta^3)$, $i \geq 1$. Hence

$$T_2(B) \geq \sum_i T_2(B_i) \geq \frac{\alpha^4}{\delta^3 2^8}\sum_i 2^{4i}|B_i|^4\,. \tag{30}$$

We have $|B| = \sum_i |B_i|$. Using the Cauchy–Schwarz inequality, we get

$$|B|^4 = \left(\sum_i |B_i| 2^i 2^{-i}\right)^4 \le \left(\sum_i 2^{4i}|B_i|^4\right) \cdot \left(\sum_i 2^{-4i/3}\right)^3 \le \sum_i 2^{4i}|B_i|^4 \,. \qquad (31)$$

Combining (31) and (30), we obtain

$$T_2(B) \ge \frac{\alpha^4}{\delta^3 2^8}|B|^4 \,. \qquad (32)$$

Let us consider the general case $k \ge 2$.

**Proof of Theorem 1.5** First of all let us prove the analog of Lemma 2.1.

**Lemma 2.2** *Let $\delta, \alpha'$ be real numbers, $0 < \alpha' \le \delta$, $A$ be a subset of $\mathbb{Z}_N$, $|A| = \delta N$ and $k \ge 2$ be an even number. Let also*

$$\mathcal{R}'_{\alpha'} = \{\ r \in \mathbb{Z}_N \ :\ \alpha' N \le |\widehat{A}(r)| < 2\alpha' N\ \} \,. \qquad (33)$$

*and $B'$ be an arbitrary subset of $\mathcal{R}'_{\alpha'} \setminus \{0\}$. Then $T_k(B') \ge \delta(\alpha')^{2k}|B'|^{2k}/(2\delta)^{2k}$.*

**Proof.** Let

$$f_{B'}(x) = \frac{1}{N}\sum_{r\in B'} \widehat{A}(r)e(rx) \,.$$

Consider the sum

$$\sigma = \left(\sum_x f_{B'}(x)A(x)\right)^k \,. \qquad (34)$$

Clearly,

$$\sigma \ge (\alpha'^2|B'|N)^k \qquad (35)$$

(see proof of Lemma 2.1). Since $k$ is even it follows that $k = 2k'$, $k' \in \mathbb{N}$. Using Hölder's inequality, we get

$$\sigma = \left(\sum_x f_{B'}(x)A(x)\right)^{2k'} \le \left(\sum_x |f_{B'}(x)|^{2k'}A^2(x)\right)\left(\sum_x A(x)\right)^{k-1} =$$

$$= \left(\sum_x |f_{B'}(x)|^{2k'}A^2(x)\right)(\delta N)^{k-1} \,. \qquad (36)$$

Hence

$$\sigma'^2 = \left(\sum_x |f_{B'}(x)|^{2k'}A^2(x)\right)^2 \ge \delta^2\frac{\alpha'^{4k}}{\delta^{2k}}|B'|^{2k}N^2 \,. \qquad (37)$$

On the other hand, using (11), we have

$$\sigma' = \sum_x |f_{B'}(x)|^{2k'}A^2(x) = \frac{1}{N^{2k'+2}}\sum_x \sum_{r_1,\dots,r_{k'},r'_1,\dots,r'_{k'}} \sum_{y,z} \widehat{f}(r_1)\dots\widehat{f}(r_{k'})\overline{\widehat{f}(r_1)}\dots\overline{\widehat{f}(r_{k'})}\widehat{A}(y)\overline{\widehat{A}(z)}$$

$$e(x(r_1+\dots+r_{k'}-r'_1-\dots-r'_{k'}))e(x(y-z)) =$$

$$= \frac{1}{N^{2k'+1}}\sum_{u,y} \sum_{r_1,\dots,r_{k'},r'_1,\dots,r'_{k'},r_1+\dots+r_{k'}=r'_1+\dots+r'_{k'}-u} \widehat{f}(r_1)\dots\widehat{f}(r_{k'})\overline{\widehat{f}(r_1)}\dots\overline{\widehat{f}(r_{k'})}\widehat{A}(y)\overline{\widehat{A}(y-u)} =$$

$$= \frac{1}{N^{2k'+1}} \sum_u \left( \sum_y \widehat{A}(y) \overline{\widehat{A}(y-u)} \right) \times$$

$$\times \left( \sum_{r_1,\ldots,r_{k'},r'_1,\ldots,r'_{k'},r_1+\cdots+r_{k'}=r'_1+\cdots+r'_{k'}-u} \widehat{f}(r_1)\ldots\widehat{f}(r_{k'})\overline{\widehat{f}(r_1)}\ldots\overline{\widehat{f}(r_{k'})} \right) \tag{38}$$

It follows that

$$\sigma'^2 \leq \frac{1}{N^{4k'+2}} \sum_u \left| \sum_y \widehat{A}(y) \overline{\widehat{A}(y-u)} \right|^2 \times$$

$$\times \sum_u \left| \sum_{r_1,\ldots,r_{k'},r'_1,\ldots,r'_{k'},r_1+\cdots+r_{k'}=r'_1+\cdots+r'_{k'}-u} \widehat{f}(r_1)\ldots\widehat{f}(r_{k'})\overline{\widehat{f}(r_1)}\ldots\overline{\widehat{f}(r_{k'})} \right|^2 = \sigma_1 \cdot \sigma_2 \,. \tag{39}$$

Using (15) and Parseval's identity, we obtain

$$\sigma_1 = N^2 \sum_u |\widehat{A}(u)|^2 = \delta N^4 \,. \tag{40}$$

Since $B' \subseteq \mathcal{R}'_{\alpha'} \setminus \{0\}$ it follows that $|\widehat{f}_{B'}(r)| \leq 2\alpha' B'(r) N$. Hence

$$\sigma_2 \leq \left( (2\alpha' N)^{2k'} \right)^2 \sum_u \left| \sum_{r_1,\ldots,r_{k'},r'_1,\ldots,r'_{k'},r_1+\cdots+r_{k'}=r'_1+\cdots+r'_{k'}-u} B'(r_1)\ldots B'(r_{k'})B'(r_1)\ldots B'(r_{k'}) \right|^2$$

$$= (2\alpha' N)^{2k} \cdot T_k(B') \,. \tag{41}$$

Using (37), (40) and (41), we get

$$T_k(B') \geq \delta(\alpha')^{2k} |B'|^{2k} / (2\delta)^{2k} \,. \tag{42}$$

This completes the proof of Lemma 2.2.

Let

$$B_i = \{\ r \in B\ :\ \alpha 2^{i-1} N \leq |\widehat{A}(r)| < \alpha 2^i N\ \}\,, \quad i \geq 1\,.$$

Clearly, $B = \bigsqcup_{i\geq 1} B_i$. Using Lemma 2.2, we obtain $T_k(B_i) \geq \delta(\alpha 2^{i-1})^{2k} |B_i|^{2k} / (2\delta)^{2k}$, $i \geq 1$. Hence

$$T_k(B) \geq \sum_i T_k(B_i) \geq \frac{\delta \alpha^{2k}}{2^{4k}\delta^{2k}} \sum_i 2^{2ki} |B_i|^{2k} \,. \tag{43}$$

We have $|B| = \sum_i |B_i|$. Using Hölder's inequality, we get

$$|B|^{2k} = \left( \sum_i |B_i| 2^i 2^{-i} \right)^{2k} \leq \left( \sum_i 2^{2ki} |B_i|^{2k} \right) \cdot \left( \sum_i 2^{-2ki/(2k-1)} \right)^{2k-1} \leq \sum_i 2^{2ki} |B_i|^{2k} \,. \tag{44}$$

Combining (44) and (43), we have

$$T_k(B) \geq \frac{\delta \alpha^{2k}}{2^{4k}\delta^{2k}} |B|^{2k} \,. \tag{45}$$

This completes the proof.

**3. Linear equations over sets of large exponential sums.**

Let $k$ be a positive interger, $d \geq 0$ be an integer. Let $M = (m_{ij})$ be a matrix $(2^{d+1}k \times (d+1))$, where elements $(m_{ij})$ of $M$ is defined by

$$m_{ij} = \begin{cases} 1, & \text{if binary expansion of } (j-1) \text{ has 1 on } (i-1) \text{ position,} \\ & \text{and } 1 \leq j \leq 2^d k\,, \\ -1, & \text{if binary expansion of } (j-1) \text{ has 1 on } (i-1) \text{ position,} \\ & \text{and } 2^d k < j \leq 2^{d+1}k\,, \\ 0, & \text{otherwise.} \end{cases}$$

Recall that binary expansion of a natural number $n$ is defined by $n = \sum n_l \cdot 2^{l-1}$, $l \geq 1$ and $n_l \in \{0,1\}$.

Let us give an example of $M$. Let $k = 2$ and $d = 2$. Then

$$M = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & -1 & -1 & -1 & -1 & -1 & -1 & -1 & -1 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & -1 & 0 & -1 & 0 & -1 & 0 & -1 \\ 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & -1 & -1 & 0 & 0 & -1 & -1 \end{pmatrix}$$

In this section we prove the following theorem.

**Theorem 3.1** *Let $\delta, \alpha$ be real numbers, $0 < \alpha \leq \delta$, $A$ be a subset of $\mathbb{Z}_N$, $|A| = \delta N$, $k$ be a positive integer, and $d \geq 0$ be an integer. Let also $B \subseteq \mathcal{R}_\alpha \setminus \{0\}$ be an arbitrary set. Consider the system of equations*

$$\sum_{i=1}^{d} \sum_{j=1}^{2^{d+1}k} m_{ij} r_j = 0\,, \tag{46}$$

*where the elements $(m_{ij})$ of $M = (m_{ij})$ was defined earlier, and $r_j \in B$. Then the number of solutions of (46) is at least*

$$\left(\frac{\delta \alpha^{2k}}{2^{4k}\delta^{2k}} |B|^{2k}\right)^{2^d}\,. \tag{47}$$

Clearly, Theorem 3.1 is a generalization of Theorem 1.5. To see this one can put $d = 0$ in Theorem 3.1.

We need in some properties of Gowers uniformity norms in our proof (see [2]).

Let $d \geq 0$ be an integer, and let $\{0,1\}^d = \{\omega = (\omega_1, \ldots, \omega_d) \,:\, \omega_j \in \{0,1\}, j = 1,2,\ldots,d\}$ be the standard discrete $d$—dimensional cube. For any $\omega \in \{0,1\}^d$ we define $|\omega| := \omega_1 + \cdots + \omega_d$. If $h = (h_1, \ldots, h_d) \in \mathbb{Z}_N^d$ we define $\omega \cdot h := \omega_1 h_1 + \ldots \omega_d h_d$. Let also $\mathcal{C}$ is the conjugation operator $\mathcal{C}f(x) := \overline{f(x)}$. By $\|\omega\|$ define the sum $\sum_{i=1}^{d} \omega_i \cdot 2^{i-1} + 1$. Let $\omega \in \{0,1\}^d$. By the same letter $\omega$ we define the map $\omega : \mathbb{Z}_N^{2^d} \to \mathbb{Z}_N$ by the rule: if $\vec{r} \in \mathbb{Z}_N^{2^d}$ then $\omega(\vec{r})$ is $\|\omega\|$–th component of the vector $\vec{r}$.

*Definition 3.2* Let $f : \mathbb{Z}_N \to \mathbb{C}$ be a function. *Gowers uniformity norm* (or Gowers norm) of $f$ is

$$\|f\|_{U^d} := \left(\frac{1}{N^{d+1}} \sum_{x \in \mathbb{Z}_N, h \in \mathbb{Z}_N^d} \prod_{\omega \in \{0,1\}^d} \mathcal{C}^{|\omega|} f(x + \omega \cdot h)\right)^{1/2^d}\,. \tag{48}$$

We need in the following lemma (see [2]).

**Lemma 3.3** *Let $f : \mathbb{Z}_N \to \mathbb{C}$ be a function, and $d$ be a positive integer. Then*

$$\|f\|_{U^d} \leq \|f\|_{U^{d+1}}\,. \tag{49}$$

Let us prove the analog of Lemma 2.2.

**Lemma 3.4** *Let $\delta, \alpha'$ be real numbers, $0 < \alpha' \le \delta$, $A$ be a subset of $\mathbb{Z}_N$, $|A| = \delta N$, $k$ be a positive integer, and $d \ge 0$ be an integer. Let also*

$$\mathcal{R}'_{\alpha'} = \{\ r \in \mathbb{Z}_N\ :\ \alpha' N \le |\widehat{A}(r)| < 2\alpha' N\ \}\,, \tag{50}$$

*and $B'$ be an arbitrary subset of $\mathcal{R}'_{\alpha'} \setminus \{0\}$. Then the number of solutions of system (46), where $r_j \in B'$ is at least*

$$\left(\frac{\delta \alpha'^{2k}}{2^{2k}\delta^{2k}}|B'|^{2k}\right)^{2^d}\,. \tag{51}$$

**Proof.** Let

$$f(x) = \frac{1}{N}\sum_{r\in B'} \widehat{A}(r)e(rx)\,.$$

Using Hölder's inequality, we get

$$\left|\sum_x f(x)A(x)\right|^{2k} \le \sum_x |f(x)|^{2k}\cdot\left(\sum_x A(x)\right)^{2k-1} = \sum_x |f(x)|^{2k}\cdot(\delta N)^{2k-1}\,. \tag{52}$$

On the other hand, using Parseval's identity and the definition of the set $\mathcal{R}'_{\alpha'}$, we have

$$\sum_x f(x)A(x) = \frac{1}{N}\sum_r \widehat{f}(r)\overline{\widehat{A}(r)} = \frac{1}{N}\sum_r |\widehat{f}(r)|^2 \ge \alpha'^2|B'|N\,. \tag{53}$$

Consider the sum

$$\sigma = \|\ |f|^{2k}\|_{U^0} = \|\ |f|^{2k}\|_{U^1} = \frac{1}{N}\sum_x |f(x)|^{2k}\,. \tag{54}$$

Combining (52) and (53), we obtain

$$\sigma \ge \frac{\delta\alpha'^{4k}}{\delta^{2k}}|B'|^{2k}\,. \tag{55}$$

Using Lemma 3.3, we get

$$\sigma^{2^d} \le \frac{1}{N^{d+1}}\sum_{x\in\mathbb{Z}_N}\sum_{h\in\mathbb{Z}_N^d}\prod_{\omega\in\{0,1\}^d}|f(x+\omega\cdot h)|^{2k} = \frac{1}{N^{d+1}}\sum_{x\in\mathbb{Z}_N}\sum_{\vec{h}\in\mathbb{Z}_N^d}\left|\prod_{\omega\in\{0,1\}^d} f(x+\omega\cdot h)\right|^{2k} \tag{56}$$

By formula (11), we have

$$\prod_{\omega\in\{0,1\}^d} f(x+\omega\cdot h) = \frac{1}{N^{2^d}}\sum_{\vec{r}\in\mathbb{Z}_N^{2^d}}\prod_{\omega\in\{0,1\}^d}\widehat{f}(\omega(\vec{r}))e(\omega(\vec{r})(x+\omega\cdot h))\,. \tag{57}$$

Hence

$$\sigma^{2^d} = \frac{1}{N^{k2^{d+1}+d+1}}\sum_{x\in\mathbb{Z}_N}\sum_{h\in\mathbb{Z}_N^d}\sum_{r^{(1)},\dots,r^{(k)},r^{(k+1)},\dots,r^{(2k)}\in\mathbb{Z}_N^{2^d}}\prod_{i=1}^{k}\prod_{\omega^{(i)}\in\{0,1\}^d}\widehat{f}(\omega^{(i)}(r^{(i)}))e(\omega^{(i)}(r^{(i)})(x+\omega^{(i)}\cdot h))$$

$$\times \prod_{i=k+1}^{2k} \prod_{\omega^{(i)}\in\{0,1\}^d} \overline{\widehat{f}(\omega^{(i)}(r^{(i)}))} e(-\omega^{(i)}(r^{(i)})(x+\omega^{(i)}\cdot h)) \tag{58}$$

Denote by $\sum$ the following system of linear equations

$$\begin{aligned}
\sum_{i=1}^{k} \sum_{\omega^{(i)}\in\{0,1\}^d} \omega^{(i)}(r^{(i)}) &= \sum_{i=k+1}^{2k} \sum_{\omega^{(i)}\in\{0,1\}^d} \omega^{(i)}(r^{(i)}) \\
\sum_{i=1}^{k} \sum_{\omega^{(i)}\in\{0,1\}^d,\ \omega_1^{(i)}=1} \omega^{(i)}(r^{(i)}) &= \sum_{i=k+1}^{2k} \sum_{\omega^{(i)}\in\{0,1\}^d,\ \omega_1^{(i)}=1} \omega^{(i)}(r^{(i)}) \\
\cdots\cdots\cdots\cdots\cdots\cdots &\quad \cdots\cdots\cdots\cdots\cdots\cdots \\
\cdots\cdots\cdots\cdots\cdots\cdots &\quad \cdots\cdots\cdots\cdots\cdots\cdots \\
\sum_{i=1}^{k} \sum_{\omega^{(i)}\in\{0,1\}^d,\ \omega_d^{(i)}=1} \omega^{(i)}(r^{(i)}) &= \sum_{i=k+1}^{2k} \sum_{\omega^{(i)}\in\{0,1\}^d,\ \omega_d^{(i)}=1} \omega^{(i)}(r^{(i)})
\end{aligned}$$

We have

$$\sigma^{2^d} = \frac{1}{N^{k2^{d+1}+d+1}} \sum_{r^{(1)},\dots,r^{(k)},r^{(k+1)},\dots,r^{(2k)}\in\mathbb{Z}_N^{2d}} \prod_{i=1}^{k} \prod_{\omega^{(i)}\in\{0,1\}^d} \widehat{f}(\omega^{(i)}(r^{(i)}))$$

$$\times \prod_{i=k+1}^{2k} \prod_{\omega^{(i)}\in\{0,1\}^d} \overline{\widehat{f}(\omega^{(i)}(r^{(i)}))} \sum_{x\in\mathbb{Z}_N} \sum_{h\in\mathbb{Z}_N^d} e(\omega^{(i)}(r^{(i)})(x+\omega^{(i)}\cdot h) - \omega^{(i)}(r^{(i)})(x+\omega^{(i)}\cdot h))$$

$$= \frac{1}{N^{k2^{d+1}}} \sum_{r^{(1)},\dots,r^{(k)},r^{(k+1)},\dots,r^{(2k)}\in\sum} \prod_{i=1}^{k} \prod_{\omega^{(i)}\in\{0,1\}^d} \widehat{f}(\omega^{(i)}(r^{(i)})) \prod_{i=k+1}^{2k} \prod_{\omega^{(i)}\in\{0,1\}^d} \overline{\widehat{f}(\omega^{(i)}(r^{(i)}))} \tag{59}$$

The vectors $r^{(1)},\dots,r^{(k)},r^{(k+1)},\dots,r^{(2k)}$ in (59) satisfy system $\sum$. It is easy to see that this system of equations is system (46).

Indeed, since $\widehat{f}_{B'}(r) = \widehat{A}(r)B'(r)$ and $B' \subseteq \mathcal{R}'_{\alpha'} \setminus \{0\}$ it follows that $|\widehat{f}_{B'}(r)| \le 2\alpha' B'(r)N$. Hence

$$\sigma^{2^d} \le (2^{2k}(\alpha')^2 k)^{2^d} N^{k2^{d+1}}\,. \tag{60}$$

Using (55), (56) and (60), we finally obtain

$$\sum_{r^{(1)},\dots,r^{(k)},r^{(k+1)},\dots,r^{(2k)}\in\sum}^{*} 1 \ge \left(\frac{\delta(\alpha')^{4k}}{\delta^{2k}}|B'|^{2k}\right)^{2^d} \frac{1}{(2^{2k}(\alpha')^{2k})^{2^d}} = \left(\frac{\delta\alpha'^{2k}}{2^{2k}\delta^{2k}}|B'|^{2k}\right)^{2^d}. \tag{61}$$

All components of all vectors in (61) belong to $B'$. In other words the number of solutions of system (46), where $r_j \in B'$ is at least

$$\left(\frac{\delta\alpha'^{2k}}{2^{2k}\delta^{2k}}|B'|^{2k}\right)^{2^d}.$$

This completes the proof of Lemma 3.4.

Let us prove Theorem 3.1.

Let

$$B_i = \{\ r\in B\ :\ \alpha 2^{i-1}N \le |\widehat{A}(r)| < \alpha 2^i N\ \}\,,\quad i\ge 1\,.$$

Clearly, $B = \bigsqcup_{i\geq 1} B_i$.

Let $E$ be a set. By $S_{k,d}(E)$ denote the number of solutions of system (46), where $r_i \in E$. Using Lemma 3.4, we get

$$S_{k,d}(B_i) \geq \left(\frac{\delta(\alpha 2^{i-1})^{2k}}{2^{2k}\delta^{2k}}|B_i|^{2k}\right)^{2^d},$$

where $i \geq 1$. Hence

$$S_{k,d}(B) \geq \sum_i S_{k,d}(B_i) \geq \left(\frac{\delta\alpha^{2k}}{2^{4k}\delta^{2k}}\right)^{2^d} \sum_i \left(2^{2ki}|B_i|^{2k}\right)^{2^d}. \tag{62}$$

We have $|B| = \sum_i |B_i|$. Using Hölder's inequality, we obtain

$$|B|^{k2^{d+1}} = \left(\sum_i |B_i| 2^i 2^{-i}\right)^{k2^{d+1}} \leq \left(\sum_i \left(2^{2ki}|B_i|^{2k}\right)^{2^d}\right) \cdot \left(\sum_i 2^{-(k2^{d+1}i)/(k2^{d+1}-1)}\right)^{k2^{d+1}-1} \leq$$

$$\leq \sum_i \left(2^{2ki}|B_i|^{2k}\right)^{2^d}. \tag{63}$$

Combining (63) and (62), we have

$$S_{k,d}(B) \geq \left(\frac{\delta\alpha^{2k}}{2^{4k}\delta^{2k}}|B|^{2k}\right)^{2^d}. \tag{64}$$

This completes the proof of Theorem 3.1.

**4. Applications.**

Chang [3] used in her proof a theorem of Rudin [21] (see also [22]) concerning dissociated subsets of $\mathbb{Z}_N$. We say that $\mathcal{D} = \{d_1, \dots, d_{|\mathcal{D}|}\} \subseteq \mathbb{Z}_N$ is *dissociated* if the equality

$$\sum_{i=1}^{|\mathcal{D}|} \varepsilon_i d_i = 0 \pmod N, \tag{65}$$

where $\varepsilon_i \in \{-1, 0, 1\}$ implies that all $\varepsilon_i$ are equal to zero.

**Theorem 4.1 (Rudin)** *There exists an absolute constant $C > 0$ such that for any dissociated set $\mathcal{D} \subseteq \mathbb{Z}_N$, any complex numbers $a_n \in \mathbb{C}$, and all positive integers $p \geq 2$ the following inequality holds*

$$\frac{1}{N}\sum_{x\in\mathbb{Z}_N}\left|\sum_{n\in\mathcal{D}} a_n e(nx)\right|^p \leq (C\sqrt{p})^p \left(\sum_{n\in\mathcal{D}}|a_n|^2\right)^{p/2}. \tag{66}$$

The proofs of Theorem 4.1 and Chang's theorem can be found in [9, 10]. Let us show that Rudin's theorem and Theorem 1.5 imply Theorem 1.1.

**Proposition 4.2** *Theorem 1.5 and Theorem 4.1 imply Theorem 1.1.*

**Proof.** Let $k = 2\lceil\log(1/\delta)\rceil$, and let $\mathcal{D} \subseteq \mathcal{R}_\alpha$ be a *maximal* dissociated subset of $\mathcal{R}_\alpha$. Since $\mathcal{D}$ is a dissociated set it follows that $0 \notin \mathcal{D}$. Using Theorem 1.5, we get

$$T_k(\mathcal{D}) \geq \frac{\delta\alpha^{2k}}{2^{4k}\delta^{2k}}|\mathcal{D}|^{2k}. \tag{67}$$

On the other hand

$$T_k(\mathcal{D}) \le C^{2k} 2^k k^k |\mathcal{D}|^k \,, \tag{68}$$

where $C$ is an absolute constant (see Theorem 4.1). Indeed, let number $a_n$ in (66) equals $\mathcal{D}(n)$, and $p = 2k$. Then the left hand side of (66) is $T_k(\mathcal{D})$, and the right hand side is equal to $C^{2k}2^k k^k |\mathcal{D}|^k$. We have $k = 2\lceil \log 1/\delta \rceil$. Using (67) and (68), we obtain $|\mathcal{D}| \le 2^8 C^2 (\delta/\alpha)^2 (\log 1/\delta)$. Since $\mathcal{D}$ is a maximal dissociated subset of $\mathcal{R}_\alpha$ it follows that any $r \in \mathcal{R}_\alpha$ can be written as $r = \sum_{i=1}^{|\mathcal{D}|} \varepsilon_i d_i \pmod N$, where $d_i \in \mathcal{D}$ and $\varepsilon_i \in \{-1, 0, 1\}$. This completes the proof of Proposition 4.2.

In the paper we obtain an improvement of Chang's result. We prove our Theorem 4.3 in the spirit of works [23, 24, 25].

**Theorem 4.3** *Let $N$ be a positive integer, $(N, 6) = 1$, $\delta, \alpha$ be real numbers, $0 < \alpha \le \delta \le 1/16$, and $A$ be a subset of $\mathbb{Z}_N$, $|A| = \delta N$. Then there exists a set $\Lambda^* \subseteq \mathbb{Z}_N$,*

$$|\Lambda^*| \le \min\big(\max(2^{30}(\delta/\alpha)^2 \log(1/\delta), 2^{4(\log\log(1/\delta))^2+2}),\ 2^{20}(\delta/\alpha)^2 \log^{13/7}(1/\delta)\big) \tag{69}$$

*such that for any residual $r \in \mathcal{R}_\alpha$ there exists a tuple $\lambda_1^*, \dots, \lambda_M^* \in \Lambda^*$, $M \le 8\log(1/\delta)$ such that*

$$r = \sum_{i=1}^{M} \varepsilon_i \lambda_i^* \pmod N \,, \tag{70}$$

*where $\varepsilon_i \in \{-1, 0, 1\}$.*

*Besides there exists a set $\tilde{\Lambda} \subseteq \mathbb{Z}_N$,*

$$|\tilde{\Lambda}| \le 2^{20}(\delta/\alpha)^2 \log^{5/3}(1/\delta) \log\log(1/\delta) \tag{71}$$

*such that for any residual $r \in \mathcal{R}_\alpha$ there exists a tuple $\tilde{\lambda}_1, \dots, \tilde{\lambda}_M \in \tilde{\Lambda}$, $M \le 8\log(1/\delta)$ such that (70) holds.*

**Corollary 4.4** *Let $N$ be a positive integer, $(N, 6) = 1$, and $\delta, \alpha$ be real numbers, $0 < \alpha \le \delta \cdot 2^{-2(\log\log(1/\delta))^2}$. Then there exists a set $\Lambda^* \subseteq \mathbb{Z}_N$, $|\Lambda^*| \le 2^{30}(\delta/\alpha)^2 \log(1/\delta)$ such that for any residual $r \in \mathcal{R}_\alpha$ there exists a tuple $\lambda_1^*, \dots, \lambda_M^* \in \Lambda^*$, $M \le 8\log(1/\delta)$ such that $r = \sum_{i=1}^{M} \varepsilon_i \lambda_i^* \pmod N$, where $\varepsilon_i \in \{-1, 0, 1\}$.*

To prove Theorem 4.3 we need in some statements and definitions.

*Definition 4.5* Let $k, s$ be positive integers. Consider the family $\Lambda(k, s)$ of subsets of $\mathbb{Z}_N$. A set $\Lambda = \{\lambda_1, \dots, \lambda_{|\Lambda|}\}$ belongs to the family $\Lambda(k, s)$ if the equality

$$\sum_{i=1}^{|\Lambda|} \lambda_i s_i = 0 \pmod N, \quad \lambda_i \in \Lambda\,, \quad s_i \in \mathbb{Z}\,, \quad |s_i| \le s\,, \quad \sum_{i=1}^{|\Lambda|} |s_i| \le 2k\,, \tag{72}$$

implies that all $s_i$ are equal to zero.

The definition of $\Lambda(k, 1)$ can be found in [26].

Note that for any $\Lambda \in \Lambda(k, s)$, we have $0 \notin \Lambda$ and $\Lambda \cap -\Lambda = \emptyset$. For an arbitrary $\Lambda \in \Lambda(k, s)$, we obtain the following upper bound for $T_k(\Lambda)$.

**Statement 4.6** *Let $k$, $s$ be positive integers, $s \ge 3$, $\Lambda$ be a subset of the family $\Lambda(k, s)$, and $|\Lambda| \ge k$. Then*

$$T_k(\Lambda) \le 2^{9k} k^k |\Lambda|^k \cdot 2^{\frac{2sk(\log k)^2}{\log(k^{2s}|\Lambda|^{s-2})}}\,. \tag{73}$$

**Example 4.7** Let $\log|\Lambda| \geq \log^2 k$, and $\Lambda$ be an arbitrary subset of the family $\Lambda(k,3)$. Using (73), we get $T_k(\Lambda) \leq 2^{20k} k^k |\Lambda|^k$.

**Proof of Statement 4.6.** Let $x \in \mathbb{Z}_N$ be a residual. By $N_k(x)$ define the number of vectors $(\lambda_1, \dots, \lambda_k)$ such that all $\lambda_i$ belong to $\Lambda$ and $\lambda_1 + \dots + \lambda_k = x$. We have $T_k(\Lambda) = \sum_{x \in \mathbb{Z}_N} N_k^2(x)$. Let $s_1, \dots, s_l$ be positive integers such that $s_1 + \dots + s_l = k$. Let

$$E(s_1, \dots, s_l)(x) = \{(\lambda_1, \dots, \lambda_k) \ : \ \text{among } \lambda_1, \dots, \lambda_k \text{ there exist exactly } s_1 \text{ residuals equals } \tilde{\lambda}_1,$$

$$s_2 \text{ residuals equals } \tilde{\lambda}_2, \dots, s_l \text{ residuals equals } \tilde{\lambda}_l \text{ such that } s_1\tilde{\lambda}_1 + \dots + s_l\tilde{\lambda}_l = x$$

$$\text{and all } \tilde{\lambda}_i \text{ are different}\}$$

Let us denote the set $E(s_1, \dots, s_l)(x)$ by $E(\vec{s})(x)$ for simplicity. Recall that for $s_1, \dots, s_l$ in the definition of $E(\vec{s})(x) = E(s_1, \dots, s_l)(x)$ the following equality holds $\sum_{i=1}^l s_i = k$. We have

$$N_k(x) = \sum_{\vec{s}} |E(\vec{s})(x)| \, .$$

It follows that

$$\sigma = T_k(\Lambda) = \sum_{x \in \mathbb{Z}_N} (\sum_{\vec{s}} |E(\vec{s})(x)|)^2 \, . \tag{74}$$

Let $\vec{s} = (s_1, \dots, s_l)$, and $G = G(\vec{s}) = \{i \ : \ s_i \leq s\}$, $B = B(\vec{s}) = \{i \ : \ s_i > s\}$. Then $|G(\vec{s})| + |B(\vec{s})| = l(\vec{s}) = l$. We have

$$l \leq k - s|B| \, . \tag{75}$$

Indeed

$$k = \sum_{i \in G} s_i + \sum_{i \in B} s_i \geq |G| + (s+1)|B| = l + s|B| \, . \tag{76}$$

Using (76) we obtain (75). Let also

$$l_j = l_j(\vec{s}) = |\, \{i \ : \ s_i = j, \ i \in [l]\}\, | \, , \qquad j = 1, 2, \dots, r = r(\vec{s}) \, .$$

Let us prove the following lemma.

**Lemma 4.8** *1) For all $\vec{s}$, $\sum_{i=1}^l s_i = k$ and for any $x \in \mathbb{Z}_N$, we have*

$$|E(\vec{s})(x)| \leq \frac{k!}{s_1! \dots s_l!} |\Lambda|^{|B(\vec{s})|} \, . \tag{77}$$

*2) For all $\vec{s}$, $\sum_{i=1}^l s_i = k$ the number of $x \in \mathbb{Z}_N$ such that $E(\vec{s})(x) \neq \emptyset$ does not exceed $|\Lambda|^l / l_1!$.*

**Proof of Lemma 4.8.** 1) Let $(\lambda_1, \dots, \lambda_k) \in E(\vec{s})(x)$ be a tuple. Then $\sum_{i=1}^k \lambda_i = \sum_{i=1}^l s_i \tilde{\lambda}_i = x$, where $\tilde{\lambda}_i \in \{\lambda_1, \dots, \lambda_k\}$ are different. Let us consider another tuple $(\lambda'_1, \dots, \lambda'_k) \in E(\vec{s})(x)$, $\sum_{i=1}^k \lambda'_i = \sum_{i=1}^l s_i \tilde{\lambda}'_i = x$, where $\tilde{\lambda}'_i \in \{\lambda'_1, \dots, \lambda'_k\}$ are different. Suppose that for all $i \in B(\vec{s})$ we have $\tilde{\lambda}_i = \tilde{\lambda}'_i$. This assumption implies that for any $i \in G(\vec{s})$ we have $\tilde{\lambda}_i = \tilde{\lambda}'_i$. Indeed $\sum_{i=1}^l s_i \tilde{\lambda}_i = x = \sum_{i=1}^l s_i \tilde{\lambda}'_i$. It follows that $\sum_{i \in G} s_i \tilde{\lambda}_i = \sum_{i \in G} s_i \tilde{\lambda}'_i$. Besides $\Lambda \cap -\Lambda = \emptyset$. Hence $\sum_{i \in G} s_i \tilde{\lambda}_i - \sum_{i \in G} s_i \tilde{\lambda}'_i = \sum_i s'_i \lambda_i^0 = 0$, where $s'_i \in \mathbb{Z}$, $|s'_i| \leq s$, $\sum_i |s'_i| \leq 2k$ and $\lambda_i^0 \in \Lambda$ are different. Using the definition of the family $\Lambda(k,s)$, we obtain that all $s'_i$ are equal to zero. It follows that for any $i \in G(\vec{s})$ we have $\tilde{\lambda}_i = \tilde{\lambda}'_i$. Hence the tuple $(\lambda'_1, \dots, \lambda'_k)$ is a permutation of $(\lambda_1, \dots, \lambda_k)$. Using the definition of the set $E(\vec{s})(x)$, we

obtain that the number of these permutations is equal to $k!/(s_1!\dots s_l!)$. It follows that the cardinality of $E(\vec{s})(x)$ does not exceed $|\Lambda|^{|B(\vec{s})|}\cdot k!/(s_1!\dots s_l!)$.

2) For any $\vec{s}$, $\sum_{i=1}^l s_i=k$ the number of $x\in\mathbb{Z}_N$ such that $E(\vec{s})(x)\neq\emptyset$ does not exceed the number of tuples $(\tilde{\lambda}_1,\dots,\tilde{\lambda}_l)$, $\sum_{i=1}^l s_i\tilde{\lambda}_i=x$, where $\tilde{\lambda}_i$ are different. Let $L_1=\{i\in[l]\ :\ s_i=1\}$. We have $|L_1|=l_1$. Consider all tuples $(\tilde{\lambda}_1,\dots,\tilde{\lambda}_l)$ and fix all $\tilde{\lambda}_i$ such that $i\notin L_1$. Note that these residuals $\tilde{\lambda}_i$ can be chosen in at most $|\Lambda|^{l-l_1}$ ways. Since all $\tilde{\lambda}_i$, $i\in L_1$ are different it follows that the number of $\tilde{\lambda}_i$ does not exceed $\binom{|\Lambda|}{l_1}\le|\Lambda|^{l_1}/l_1!$. It follows that the number of all tuples $(\tilde{\lambda}_1,\dots,\tilde{\lambda}_l)$, $\sum_{i=1}^l s_i\tilde{\lambda}_i=x$, where $\tilde{\lambda}_i$ are different at most $|\Lambda|^{l-l_1}|\Lambda|^{l_1}/l_1!=|\Lambda|^l/l_1!$. This completes the proof of Lemma 4.8.

Let $t=(k\log k)/\log(k^{2s}|\Lambda|^{s-2})$. Let us estimate the sum $\sigma$.

$$\sigma\le 2\left(\sum_{x\in\mathbb{Z}_N}\left(\sum_{\vec{s}:|B(\vec{s})|\le t}|E(\vec{s})(x)|\right)^2+\sum_{x\in\mathbb{Z}_N}\left(\sum_{\vec{s}:|B(\vec{s})|>t}|E(\vec{s})(x)|\right)^2\right)=2\sigma_1+2\sigma_2\,. \tag{78}$$

We have

$$\sigma_2\le\sum_{\vec{s}_1,\vec{s}_2:|B(\vec{s}_1)|>t,|B(\vec{s}_2)|>t}\sum_x|E(\vec{s}_1)(x)|\cdot|E(\vec{s}_2)(x)| \tag{79}$$

If $|B(\vec{s}_1)|>|B(\vec{s}_2)|$ then put $\vec{s}^*=\vec{s}_1$. If $|B(\vec{s}_1)|\le|B(\vec{s}_2)|$ then set $\vec{s}^*=\vec{s}_2$. Let also $P_k(\vec{s})=k!/(s_1!\dots s_l!)$. Using Lemma 4.8, we obtain $|E(\vec{s}_1)(x)|\le P_k(\vec{s}_1)|\Lambda|^{|B(\vec{s}^*)|}$ and $|E(\vec{s}_2)(x)|\le P_k(\vec{s}_2)|\Lambda|^{|B(\vec{s}^*)|}$. Using the same lemma one more, we get

$$\sigma_2\le\sum_{\vec{s}_1,\vec{s}_2:|B(\vec{s}_1)|>t,|B(\vec{s}_2)|>t}|\Lambda|^{l(\vec{s}^*)}|\Lambda|^{2|B(\vec{s}^*)|}P_k(\vec{s}_1)P_k(\vec{s}_2)\,. \tag{80}$$

By (75), we have

$$\sigma_2\le\sum_{\vec{s}_1,\vec{s}_2:|B(\vec{s}_1)|>t,|B(\vec{s}_2)|>t}|\Lambda|^{k-s|B(\vec{s}^*)|}|\Lambda|^{2|B(\vec{s}^*)|}P_k(\vec{s}_1)P_k(\vec{s}_2)\le \tag{81}$$

$$\le|\Lambda|^k|\Lambda|^{-t(s-2)}\sum_{\vec{s}_1,\vec{s}_2}P_k(\vec{s}_1)P_k(\vec{s}_2)\le 2^4|\Lambda|^k|\Lambda|^{-t(s-2)}(k^k)^2\,. \tag{82}$$

Since $t=(k\log k)/\log(k^{2s}|\Lambda|^{s-2})$ it follows that

$$k^k|\Lambda|^{-t(s-2)}\le 2^{\frac{2sk(\log k)^2}{\log(k^{2s}|\Lambda|^{s-2})}}\,. \tag{83}$$

Hence

$$\sigma_2\le 2^4k^k|\Lambda|^k2^{\frac{2sk(\log k)^2}{\log(k^{2s}|\Lambda|^{s-2})}}\,. \tag{84}$$

Let us estimate $\sigma_1$.

$$\sigma_1\le 2\left(\sum_{x\in\mathbb{Z}_N}\left(\sum_{\vec{s}:|B(\vec{s})|\le t,l(\vec{s})\le k-st}|E(\vec{s})(x)|\right)^2+\sum_{x\in\mathbb{Z}_N}\left(\sum_{\vec{s}:|B(\vec{s})|\le t,l(\vec{s})>k-st}|E(\vec{s})(x)|\right)^2\right)=$$

$$=2\sigma_1^{'}+2\sigma_1^{''}\,. \tag{85}$$

We have

$$\sigma_1^{'}\le\sum_{\vec{s}_1,\vec{s}_2:|B(\vec{s}_1)|,|B(\vec{s}_2)|\le t,\ l(\vec{s}_1),l(\vec{s}_2)\le k-st}\sum_x|E(\vec{s}_1)(x)|\cdot|E(\vec{s}_2)(x)| \tag{86}$$

Using Lemma 4.8 and inequality (83), we obtain

$$\sigma_1^{'} \le \sum_{\vec{s}_1,\vec{s}_2:|B(\vec{s}_1)|,|B(\vec{s}_2)|\le t,\ l(\vec{s}_1),l(\vec{s}_2)\le k-st} |\Lambda|^{l(\vec{s}^*)}|\Lambda|^{2|B(\vec{s}^*)|}P_k(\vec{s}_1)P_k(\vec{s}_2) \le \tag{87}$$

$$\le 2^4|\Lambda|^k|\Lambda|^{-t(s-2)}(k^k)^2 \le 2^4k^k|\Lambda|^k 2^{\frac{2sk(\log k)^2}{\log(k^{2s}|\Lambda|^{s-2})}}\,. \tag{88}$$

We need in upper bound for $\sigma_1^{''}$. For any $\vec{s}=(s_1,\dots,s_l)$, $\sum_{i=1}^l s_i = k$, we have

$$l_1+\dots+l_r = l \quad \text{and} \quad l_1+2l_2+\dots+rl_r = k\,. \tag{89}$$

Using (89), we get $l = k-(l_2+2l_3+\dots+(r-1)l_r)$. On the other hand $l \ge k-st$. It follows that $l_2+2l_3+\dots+(r-1)l_r \le st$. Further $l_2+\dots+l_r \le l_2+2l_3+\dots+(r-1)l_r \le st$ and $l_1 = l-(l_2+\dots+l_r) \ge l-st \ge k-2st$. Using Lemma 4.8 and (75), we get

$$\sigma_1^{''} \le \sum_{\vec{s}_1,\vec{s}_2:|B(\vec{s}_1)|,|B(\vec{s}_2)|\le t,l(\vec{s}_1),l(\vec{s}_2)>k-st} \sum_x |E(\vec{s}_1)(x)|\cdot|E(\vec{s}_2)(x)| \le \tag{90}$$

$$\le \sum_{\vec{s}_1,\vec{s}_2:|B(\vec{s}_1)|,|B(\vec{s}_2)|\le t,\ l(\vec{s}_1),l(\vec{s}_2)>k-st} \frac{|\Lambda|^{l(\vec{s}^*)}|\Lambda|^{2|B(\vec{s}^*)|}}{l_1(\vec{s}^*)!}P_k(\vec{s}_1)P_k(\vec{s}_2) \le \tag{91}$$

$$\le \sum_{\vec{s}_1,\vec{s}_2:|B(\vec{s}_1)|,|B(\vec{s}_2)|\le t,\ l(\vec{s}_1),l(\vec{s}_2)>k-st} \frac{|\Lambda|^{k-s|B(\vec{s}^*)|}|\Lambda|^{2|B(\vec{s}^*)|}}{l_1(\vec{s}^*)!}P_k(\vec{s}_1)P_k(\vec{s}_2)\,. \tag{92}$$

Since $l_1 = l_1(\vec{s}^*) \ge k-2st$ it follows that

$$\sigma_1^{''} \le \frac{|\Lambda|^k}{[k-2st]!}\sum_{\vec{s}_1,\vec{s}_2} P_k(\vec{s}_1)P_k(\vec{s}_2) \le 2^4\frac{|\Lambda|^k}{[k-2st]!}(k^k)^2\,. \tag{93}$$

By assumption $|\Lambda| \ge k$. Hence $t \le k/(3s-2)$. Using the last inequality, we have

$$[k-2st]! \ge [k-2st]^{[k-2st]}/e^k \ge k^{[k-2st]}/(8e)^k\,.$$

Since $t = (k\log k)/\log(k^{2s}|\Lambda|^{s-2})$ it follows that $k^{2st} \le 2^{\frac{2sk(\log k)^2}{\log(k^{2s}|\Lambda|^{s-2})}}$. Further

$$[k-2st]! \ge k^k/(2^{5k}2^{\frac{2sk(\log k)^2}{\log(k^{2s}|\Lambda|^{s-2})}})\,.$$

Hence

$$\sigma_1^{''} \le 2^4 2^{5k}k^k|\Lambda|^k\cdot 2^{\frac{2sk(\log k)^2}{\log(k^{2s}|\Lambda|^{s-2})}}\,. \tag{94}$$

Combining (84), (88) and (94), we finally obtain

$$\sigma = T_k(\Lambda) \le 2^{9k}k^k|\Lambda|^k\cdot 2^{\frac{2sk(\log k)^2}{\log(k^{2s}|\Lambda|^{s-2})}}\,. \tag{95}$$

This completes the proof of Statement 4.6.

**Proof of Theorem 4.3** Let $k = 2\lceil\log(1/\delta)\rceil$. Let $\Lambda = \{\lambda_1,\dots,\lambda_{|\Lambda|}\}$ be a maximal subset $\mathcal{R}_\alpha\setminus\{0\}$ belongs to the family $\Lambda(k,3)$. Let $\Lambda^* = (\bigcup_{j=1}^3 j^{-1}\Lambda)\bigcup\{0\}$. Then $|\Lambda^*| \le 4|\Lambda|$ and $0\in\Lambda^*$. Let us proof that for any $x\in\mathcal{R}_\alpha\setminus\{0\}$ there exists $j\in[s]$ such that

$$xj = \sum_{i=1}^{|\Lambda|}\lambda_i s_i\,, \qquad s_i\in\mathbb{Z}\,, \quad |s_i|\le s\,, \quad \sum_{i=1}^{|\Lambda|}|s_i| \le 2k\,. \tag{96}$$

Since for any $i \in [|\Lambda|]$, $j \in [s]$ we have $j^{-1}\lambda_i \in \Lambda^*$ it follows that (96) implies the theorem. Thus, let $x$ be an element of $\mathcal{R}_\alpha \setminus \Lambda$, $x \neq 0$. Let us consider all equations $\sum_{i=1}^{|\Lambda|+1} \tilde{\lambda}_i s_i = 0$, where $\tilde{\lambda}_i \in \Lambda \bigsqcup \{x\}$ and $s_i \in \mathbb{Z}$, $|s_i| \leq s$, $\sum_{i=1}^{|\Lambda|+1} |s_i| \leq 2k$. If all these equations are trivial i.e. we have $s_i = 0$, $i \in [|\Lambda|+1]$ then we obtain a contradiction with maximality of $\Lambda$. It follows that there exists non–trivial equation (96) such that not all numbers $j, s_1, \dots, s_{|\Lambda|}$ are equal to zero. At the same time $j \in [-s, \dots, s]$. Since $\Lambda$ belongs to the family $\Lambda(k,3)$ it follows that $j \neq 0$. Hence we can assume that $j \in [s]$. Since $2k \leq 8\log(1/\delta)$ it follows that for any $x \in \mathcal{R}_\alpha$ there exists a tuple $\lambda_1^*, \dots, \lambda_M^* \in \Lambda^*$, $M \leq 8\log(1/\delta)$ such that (70) holds.

Let us obtain the bound $|\Lambda^*| \leq \max(\, 2^{30}(\delta/\alpha)^2 \log(1/\delta), 2^{4(\log\log(1/\delta))^2+2}\,)$.

If $\log|\Lambda| < (\log k)^2$ then $|\Lambda| \leq 2^{4(\log\log(1/\delta))^2}$ and $|\Lambda^*| \leq 2^{4(\log\log(1/\delta))^2+2}$. Let $\log|\Lambda| \geq (\log k)^2$. Using Statement 4.6, we get $T_k(\Lambda) \leq 2^{20k} k^k |\Lambda|^k$. On the other hand, using Theorem 1.5, we obtain $T_k(\Lambda) \geq \delta\alpha^{2k}|\Lambda|^{2k}/(2^{4k}\delta^{2k})$. It follows that $|\Lambda| \leq 2^{27}(\delta/\alpha)^2\log(1/\delta)$ and $|\Lambda^*| \leq 2^{30}(\delta/\alpha)^2\log(1/\delta)$.

In any case, we have $|\Lambda^*| \leq \max(\, 2^{30}(\delta/\alpha)^2 \log(1/\delta), 2^{4(\log\log(1/\delta))^2+2}\,)$.

Let us prove that $|\Lambda^*| \leq 2^{20}(\delta/\alpha)^2\log^{13/7}(1/\delta)$. If $|\Lambda| < k$ then $|\Lambda^*| \leq 4|\Lambda| \leq 4k$ as required. Let $|\Lambda| \geq k$. Using Statement 4.6, we get

$$T_k(\Lambda) \leq 2^{9k} k^k |\Lambda|^k 2^{\frac{6k\log^2 k}{\log(k^6|\Lambda|)}} \leq 2^{9k} k^k |\Lambda|^k 2^{\frac{6k\log k}{7}} = 2^{9k} k^k |\Lambda|^k k^{\frac{6k}{7}}\,. \qquad (97)$$

On the other hand, by Theorem 1.5, we have $T_k(\Lambda) \geq \delta\alpha^{2k}|\Lambda|^{2k}/(2^{4k}\delta^{2k})$. It follows that $|\Lambda| \leq 2^{18}(\delta/\alpha)^2\log^{13/7}(1/\delta)$ and $|\Lambda^*| \leq 2^{20}(\delta/\alpha)^2\log^{13/7}(1/\delta)$.

Let us prove the existence of the set $\tilde{\Lambda}$. Let $s = [\log\log(1/\delta)]$ and $\Lambda_1$ be a maximal subset of $\mathcal{R}_\alpha \setminus \{0\}$ such that $\Lambda_1$ belongs to the family $\Lambda(k,s)$, $k = 2\lceil\log(1/\delta)\rceil$. Let $\tilde{\Lambda} = \bigcup_{j=1}^s j^{-1}\Lambda_1$. We have $|\tilde{\Lambda}| \leq s|\Lambda_1|$. It is easy to see that for any $r \in \mathcal{R}_\alpha$ there exists a tuple $\tilde{\lambda}_1, \dots, \tilde{\lambda}_M \in \tilde{\Lambda}$, $M \leq 8\log(1/\delta)$ such that (70) holds.

Finally, let us prove (71). If $|\Lambda_1| < k$ then we are done. Let $|\Lambda_1| \geq k$. Using Statement 4.6, we get

$$T_k(\Lambda) \leq 2^{9k} k^k |\Lambda|^k \cdot 2^{\frac{2sk\log^2 k}{\log(k^{2s}|\Lambda|^{s-2})}} \leq 2^{9k} k^k |\Lambda|^k \cdot 2^{\frac{2sk\log k}{3s-2}} = 2^{9k} k^k |\Lambda|^k k^{\frac{2sk}{3s-2}}\,. \qquad (98)$$

On the other hand, by Theorem 1.5, we have $T_k(\Lambda) \geq \delta\alpha^{2k}|\Lambda|^{2k}/(2^{4k}\delta^{2k})$. It follows that $|\Lambda| \leq 2^{20}(\delta/\alpha)^2\log^{5/3}(1/\delta)$ and $|\tilde{\Lambda}| \leq 2^{20}(\delta/\alpha)^2\log^{5/3}(1/\delta)\log\log(1/\delta)$. This completes the proof.

Let us obtain an application of Theorems 1.5 and 4.3.

Let $K$ be a subset of $\mathbb{Z}_N$ and $\varepsilon \in (0,1)$ be a real number. The *Bohr set* $B(K,\varepsilon)$ is defined to be the set

$$B(K,\varepsilon) = \{x \in \mathbb{Z}_N \ :\ \left\|\frac{rx}{N}\right\| < \varepsilon\,,\ \text{for all } r \in K\}\,,$$

where $\|\cdot\|$ is the distance to the nearest integer. Properties of Bohr sets can be found in J. Bourgain's paper [27]. In particular Bourgain proved that

$$|B(K,\varepsilon)| \geq \frac{1}{2}\varepsilon^{|K|}N\,. \qquad (99)$$

In proof of Freiman's Theorem [3] (see also [10]) Chang used the following proposition.

**Proposition 4.9** *Let $N$ be a positive integer, $\delta \in (0,1)$ be a real number, and $A$ be a subset of $\mathbb{Z}_N$, $|A| = \delta N$. Then $2A - 2A$ contains some Bohr set $B(K,\varepsilon)$, where $|K| \leq 8\delta^{-1}\log(1/\delta)$ and $\varepsilon = \delta/(2^8\log(1/\delta))$.*

We obtain the following improvement of Proposition 4.9.

**Proposition 4.10** *Let $N$ be a positive integer, $(N,6)=1$, let $0<\delta\le 2^{-256}$ be a real number, and let $A$ be a subset of $\mathbb{Z}_N$, $|A|=\delta N$. Then $2A-2A$ contains some Bohr set $B(K,\varepsilon)$, where $|K|\le 2^{33}\delta^{-1}\log(1/\delta)$ and $\varepsilon=1/(2^8\log(1/\delta))$.*

Using (99) we get the cardinality of the Bohr set $B(K,\varepsilon)$ in Proposition 4.9 is at least $(1/2)\cdot 2^{-8\delta^{-1}(\log 1/\delta)^2}N$. In Proposition 4.10 the cardinality of the Bohr set is at least $(1/2)\cdot 2^{-2^{35}\delta^{-1}(\log 1/\delta)(\log\log 1/\delta)}N$.

We need in the following definition.

*Definition 4.11* Let $f,g:\mathbb{Z}_N\to\mathbb{C}$ be arbitrary functions. We define the *convolution* $(f*g)(x)$ of the functions $f$ and $g$ by the formula

$$(f*g)(x)=\sum_{y\in\mathbb{Z}_N}f(y)g(y-x)\,. \qquad (100)$$

It is easy to check

$$\widehat{(f*g)}(r)=\widehat{f}(r)\overline{\widehat{g}(r)}\,. \qquad (101)$$

**Proof of Proposition 4.10.** Let $\alpha=\delta^{3/2}/2\sqrt{2}$. Using Corollary 4.4 we find the set $\Lambda^*\subseteq\mathbb{Z}_N$, $|\Lambda^*|\le 2^{33}\delta^{-1}\log(1/\delta)$ such that for any $r\in\mathcal{R}_\alpha$ there exists a tuple $\lambda_1^*,\dots,\lambda_M^*\in\Lambda^*$, $M\le 8\log(1/\delta)$ such that (70) holds. Let $\mathcal{R}_\alpha^*=\mathcal{R}_\alpha\setminus\{0\}$. Let us consider $B_1=B(\mathcal{R}_\alpha^*,1/20)$. For all $x\in B_1$ and any $r\in\mathcal{R}_\alpha^*$ we have

$$|1-e(rx)|=2|\sin(\pi rx/N)|\le\frac{2\pi}{20}<\frac{1}{2}\,. \qquad (102)$$

Clearly, the expression $(A*A*A*A)(x)$ is the number of quadruples $(a_1,a_2,a_3,a_4)\in A^4$ such that $a_1+a_2-a_3-a_4=x$. It follows that, $(A*A*A*A)(x)>0$ if and only if $x\in 2A-2A$. Using (11) and (101), we obtain $x\in 2A-2A$ if and only if $\sum_r|\widehat{A}(r)|^4e(rx)>0$. Let $x\in B_1$. Then

$$\sum_r|\widehat{A}(r)|^4e(rx)=\sum_r|\widehat{A}(r)|^4-\sum_r|\widehat{A}(r)|^4(1-e(rx))>\frac{1}{2}\sum_r|\widehat{A}(r)|^4-2\sum_{r\notin R,r\ne 0}|\widehat{A}(r)|^4\ge$$

$$\ge\frac{1}{2}\delta^4N^4-2\max_{r\notin R,r\ne 0}|\widehat{A}(r)|^2\sum_r|\widehat{A}(r)|^2\ge\frac{1}{2}\delta^4N^4-2\frac{\delta^3N^2}{8}\delta N^2=\frac{\delta^4N^4}{4}>0\,. \qquad (103)$$

(we have used Parseval's identity (2)). Inequality (103) implies that the set $B_1$ belongs to $2A-2A$. Let us consider another Bohr set $B_2=B(\Lambda^*,1/(2^8\log(1/\delta))$ and let us prove $B_2\subseteq B_1$. Since for any $r\in\mathcal{R}_\alpha^*$ there exists a tuple $\lambda_1^*,\dots,\lambda_M^*\in\Lambda^*$, $M\le 8\log(1/\delta)$ such that (70) holds it follows that for all $x\in B_2$, we have

$$\left\|\frac{rx}{N}\right\|\le\sum_{i=1}^M\left\|\frac{\lambda_i^*x}{N}\right\|\le 8\log(1/\delta)\cdot\frac{1}{2^8\log(1/\delta)}<\frac{1}{20}\,. \qquad (104)$$

Thus $B_2\subseteq B_1$ and we have found the Bohr set $B_2\subseteq 2A-2A$ with the required properties. This completes the proof of Proposition 4.10.

# References


[1] *Gowers W. T.* Rough structure and classification // Geom. Funct. Anal., Special Volume - GAFA2000 "Visions in Mathematics", Tel Aviv, (1999) Part I, 79–117.

[2] *Gowers W. T.* A new proof of Szemerédi's theorem // Geom. Funct. Anal. **11** (2001), 465–588.

[3] *Chang M.– C.,* A polynomial bound in Freiman's theorem // Duke Math. J. **113** (2002) no. 3, 399–419.

[4] *Ruzsa I.* Generalized arithmetic progressions and sumsets // Acta Math. Hungar. **65** (1994), 379–388.

[5] *Bilu Y.* Structure of sets with small sumset // Structure Theory of Sets Addition, Astérisque, Soc. Math. France, Montrouge, **258** (1999), 77–108.

[6] *Freiman G. A.* Foundations of a Structural Theory of Set Addition / Kazanskii Gos. Ped. Inst., Kazan, 1966. Translations of Mathimatical Monographs **37**, AMS, Providence, R.I., USA.

[7] *Green B.* Arithmetic Progressions in Sumsets // Geom. Funct. Anal. **12** (2002) no. 3, 584–597.

[8] *Green B.* Some constructions in the inverse spectral theory of cyclic groups // Comb. Prob. Comp. **12** (2003) no. 2, 127–138.

[9] *Green B.* Spectral structure of sets of integers // Fourier analysis and convexity (survey article, Milan 2001), Appl. Numer. Harmon. Anal., Birkhauser Boston, Boston, MA (2004), 83–96.

[10] *Green B.* Structure Theory of Set Addition // ICMS Instructional Conference in Combinatorial Aspects of Mathematical Analysis, Edinburgh March 25 — April 5 2002.

[11] *Bourgain J.* On Aritmetic Progressions in Sums of Sets of Integers // A Tribute of Paul Erdös, Cambridge University Press, Cambridge (1990), 105–109.

[12] *Freiman G. A., Halberstam H., Ruzsa I.* Integer Sumsets Containing Long Arithmetic Progressions // J. London Math. Soc. **46** (1992) no. 2, 193–201.

[13] *Croot E., Ruzsa I., Tomasz S.* Arithmetic progressions in sparse sumsets // preprint.

[14] *Yudin A. A.* On the measure of large values of a trigonametric sum // Number Theory (under the edition of G.A. Freiman, A.M. Rubinov, E.V. Novosyolov), Kalinin State Univ., Moscow (1973), 163–174.

[15] *Besser A.* Sets of integers with large trigonometric sums // Astérisque **258** (1999), 35–76.

[16] *Lev V. F.* Linear Equations over $\mathbb{F}_p$ and Moments of Exponential Sums // Duke Mathematical Journal **107** (2001), 239–263.

[17] *Konyagin S. V., Lev V. F.* On the distribution of exponential sums // Integers: Electronic Journal of Combinatorial Number Theory **0** # A01, (2000).

[18] *de Leeuw K., Katznelson Y., Kahane J. P.* Sur les coefficients de Fourier des fonctions continues // C. R. Acad. Sci. Paris Sér. A–B **285** (1977) no. 16, A1001–A1003.

[19] *Nazarov F. L.* The Bang solution of coefficient problem // Algebra i Analiz **9** (1997) no. 2, 272–287. English Transl. in St. Petersburg Math. J. **9** (1998) no. 2, 407–419.

[20] *Ball K.* Convex geometry and functional analysis // Handbook of the geometry of Banach spaces, vol. I, North–Holland, Amsterdam (2001), 161–194.

[21] *Rudin W.* Fourier analysis on groups / Wiley 1990 (reprint of the 1962 original).

[22] *Rudin W.* Trigonometric series with gaps // J. Math. Mech. **9** (1960), 203–227.

[23] *Vinogradov I. M.* The method of trigonometric sums in number theory / M.: Nauka, 1971.

[24] *Linnik Y. V.* On Weyl's sums. // Math. Sbornik **12** (1943) . I, 28–39.

[25] *Nesterenko Y. V.* On I.M. Vinogradov's mean–value theorem // Trudi of Moscow Math. Soc. **48** (1985), 97–105.

[26] *Bajnok B., Ruzsa I.* The independence number of a subset of an abelian group // Integers: Electronic Journal of Combinatorial Number Theory **3** # A02, 2003.

[27] *Bourgain J.* On triples in arithmetic progression // Geom. Funct. Anal. **9** (1999), 968–984.